What to look for in a DRaaS Solution

Storage Switzerland, LLC

GEORGE CRUMP
LEAD ANALYST—STORAGE SWITZERLAND

WHAT TO LOOK FOR IN A DRAAS SOLUTION

Disaster Recovery as a Service (DRaaS) outsources and simplify simplifies the most difficult situations that an IT Team will ever face; recovering their organization's servers and applications in the event of a disaster. Instead of having to maintain a recovery site, DRaaS allows the organization to leverage a cloud backup service provider's cloud to recover servers in that cloud and in some cases via a cloud backup appliance. DRaaS should lower DR costs and dramatically simplify the DR process. As a result, the number of companies claiming to provide DRaaS has grown exponentially over the past year. Now the challenge facing IT professionals is selecting the right DRaaS vendor because the capabilities and pricing vary wildly between each.

Most DRaaS vendors started out as cloud backup suppliers and have added the capability as part of their service. It is important for the IT professional to understand that their relationship with a DRaaS provider is fundamentally different than with a cloud backup supplier. The cloud backup vendor has a relatively low bar of responsibility compared to a DRaaS vendor. The cloud backup vendor is merely providing a second or even third copy of data. The only time that this relationship is vital is when the business needs to recover data in a relatively short time frame. The DRaaS vendor on the other hand is providing not only the ability to recover data, but also to run that application when there is a server, storage or data center failure. The DRaaS provider has the responsibility to provide enough compute and storage performance as well as reliable network connectivity so that that application, when recovered, is also usable.

Five Things To Look For in a DRaaS Solution

01

RECOVERY TIMES AND PROCESSES THAT MEET THE ORGANIZATION'S EXPECTATIONS

The number one aspect of DRaaS to look for is a provider that can meet the organization's expectations for recovery. While most DRaaS vendors will claim that they can run the application in their cloud, few provide exact details on either what the recovery process looks like, or how long it will actually take. "Instant", it turns out, seems to be a relative term. The time to recover can range from a few minutes to multiple hours.

DRaaS recovery times can be impacted by two key factors. The first factor is what is involved in initiating a recovery in their cloud. Some providers require that the vendor's staff manually position the application to be recovered while others allow the customer to trigger

the recovery directly from their GUI. The problem with the manual process is that this means that calls or emails need to be sent from the DRaaS customer, and personnel at the other end need to be available and be able to drop whatever they were working on to initiate the recovery. A self-service recovery allows the restoration of applications to begin the moment the customer wants without sending emails or making phone calls, a far more efficient process.

The second factor to consider is the process involved in preparing the application and cloud environment to move from backing up an application to hosting one. This may mean moving the application from its backup state to a live state, essentially in the time it takes to recover the application in their data center. It may also mean potentially moving that application from a backup infrastructure to a compute infrastructure. How these processes occur really shouldn't matter to the DRaaS customer, instead they should pay attention to the time it takes from initiation of recovery request to live and accessible applications.

02

SIMPLE FAIL BACK STRATEGY

A second thing to look for in a DRaaS provider is a well thought out fail-back strategy when the original data center is restored to operation. Some providers have the ability to restore an application while the production version is running in their cloud and then do a "quick-sync" of data to push the final changes to the application. This method is fine for most applications, but for applications with large data sets it could take weeks for this process to complete, depending on the available bandwidth. If the business has a large application they plan to use in their DRaaS strategy then another form of transport may be needed, potentially shipping hard disk drives or tape media. Then the data can be overnighted to the data center, restored and then again quick-sync final updates.

03

FLEXIBLE RECOVERY

There are two types of disasters, major and minor. A major disaster is typically top of mind. It involves the total inaccessibility of the data center which is typically caused by some natural event like hurricane, flood, fire or earthquake. These disasters are often regional in nature, impacting a wide variety of businesses. The other type of disaster is a minor disaster, impacting a specific application. These are often caused by a corruption of the application's data, or a failure of the

server or its storage. While not as dramatic as a wide spread disaster, these minor disasters are far more common, impacting every business multiple times a year.

In the case of these minor disasters, the data center is still intact and highly functional. Just a component in that data center has failed. Failing to the cloud introduces the recovery situation discussed above. As Storage Switzerland discussed in the article, "What is Hybrid Cloud Backup?", many cloud backup solutions leverage an on-site appliance to store a local copy of data in addition to a cloud copy. For a minor disaster it makes more sense to leverage this on-site appliance as a host for the application instead of the cloud. The hybrid appliance typically provides its own storage and compute so it should be immune from whatever failure caused the application outage.

The problem is that not all DRaaS providers can leverage the appliance for recovery and hosting of an application. It is critical to ask the DRaaS supplier if this is possible as it is the most logical place to recover and host an application in the event of a minor failure.

Another aspect of flexible recovery is to consider exactly what can be recovered. Many DRaaS providers can only host virtual machines that have already been virtualized and are being backed up as virtual machines. Some providers even require that a specific hypervisor be used, typically VMware. While VMware is certainly the hypervisor market leader, Hyper-V and Linux based hypervisor solutions are gaining popularity quickly. It is important to look for a DRaaS solution that can backup, recover AND host bare metal servers across a variety of operating systems as well as virtual machines from multiple hypervisors.

04

PERFORMANCE IMPACT

Another important question to ask is what will the performance of the system look like when a disaster is declared? Many DRaaS service level agreements (SLAs) do not specify what the performance of the application will be during their hosting of it. This is a very important aspect of DRaaS to understand. Recovery is important and while exact production performance is not required, the application does have to be usable. In fact, the worse the performance of the cloud hosted application is, the more pressure there is on IT to re-establish the data center quickly.

To address this issue many DRaaS providers limit the number of applications that a customer can instantiate at any given time. While this may not be an issue for some environments, many may require the need to have a dozen or more covered by the DRaaS strategy. It is important to understand what these limits are before entering into a relationship with the provider.

05

COSTS

Potentially the most confusing part of establishing a DRaaS strategy is understanding how the pricing structure will work. There are so many ways to present these costs that it can be overwhelming. Look for a provider that can deliver a simple and easy to understand pricing model. That model should include the price per recovered server or application, a cost or provision for a certain amount of testing per year and any associated costs to restore data. There may also be an up-charge to run the application in the provider's cloud for an extended period of time.

Conclusion

DRaaS can provide many benefits to data centers of all sizes. The cost savings by not having to maintain a secondary disaster recovery site and a recovery infrastructure can be significant. But the costs associated with DRaaS as well as its ability to deliver on user expectations vary wildly between providers. It is important to look for a solution that can deliver timely and self-service recovery, leverage on-site copies of data for recovery and not require 100% virtualization in order to be effective.

Storage Switzerland, LLC

Storage Switzerland is the leading storage analyst firm focused on the emerging storage categories of memory-based storage (Flash), Big Data, virtualization, and cloud computing. The firm is widely recognized for its blogs, white papers, and videos on current approaches such as all-fash arrays, deduplication, SSDs, software-defined storage, backup appliances, and storage networking. The name "Storage Switzerland" indicates a pledge to provide neutral analysis of the storage marketplace, rather than focusing on a single vendor or approach.

Disaster Recovery as a Service Checklist

Backup:

☐ Does the solution protect all your key platforms and applications?

☐ Does the solution create a local copy in addition to the cloud?

☐ Does the solution intelligently manage the size of the local copy?

Recovery:

☐ What is the total application recovery time? _____

☐ Is DRaaS Self-Service? _____

☐ What is involved to move from a backup to live state?

☐ Have you clarified potential networking issues?

☐ What operating systems can be recovered?

☐ Can the local appliance be used for recovery?

Failed-State:

☐ What are the performance guaranteed while hosted in the DRaaS Cloud?

☐ What architecture does the provider have to meet this guarantee?

☐ What are the maximum number of VMs that the DRaaS will allow?

Failback:

☐ How long will the provider host your VMs? Penalty for extended time?

☐ How does the vendor manage failback (data shipping, reverse replicate)?

☐ Is there expectation of data loss during failback?

☐ Is there expectation of downtime during failback? _____